# FortiAuthenticator - Release Notes

VERSION 5.5.0

**FORTINET DOCUMENT LIBRARY**

https://docs.fortinet.com

**FORTINET VIDEO GUIDE**

https://video.fortinet.com

**FORTINET KNOWLEDGE BASE**

http://kb.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTINET COOKBOOK**

http://cookbook.fortinet.com

**FORTINET NSE INSTITUTE (TRAINING)**

https://training.fortinet.com/

**FORTIGUARD CENTER**

https://fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**END USER LICENSE AGREEMENT AND PRIVACY POLICY**

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

**FEEDBACK**

Email: techdocs@fortinet.com

November 19, 2018

FortiAuthenticator - Release Notes

23-550-522805-20181119

# TABLE OF CONTENTS

# Introduction

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator™ 5.5.0, build 0366.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit:

http://docs.fortinet.com/fortiauthenticator/

# Special notices

## Upgrading an existing FortiAuthenticator KVM instance

Due to security enhancements in FortiAuthenticator 5.5.0, users upgrading an existing KVM instance to this firmware version are advised to reconfigure their FortiAuthenticator instances to ensure they include the presence of an emulated HWRNG device.

A GUI management tool such as virt-manager may be used to modify the VM settings to add the emulated HWRNG device (*Add Hardware* > *RNG*). Alternatively, you can modify the VM's XML description to add the following code inside the <devices>…</devices> section:

```
<rng model='virtio'>
   <backend model='random'>/dev/urandom</backend>
   <address type='pci' domain='0x0000' bus='0x00' slot='0x0d' function='0x0'/>
</rng>
```

## TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

## Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the web-based manager to be viewed properly without need for scrolling.

## Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to **System > Dashboard > Status** and select **Backup/Restore > Download backup file** to backup the configuration.

## After any upgrade

If you are using the web-based manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the web-based manager screens are displayed properly.

# What's new in FortiAuthenticator 5.5

Note that this is a patch release. See Resolved issues and Known issues for more information.

For more detailed information, see the FortiAuthenticator 5.5 Administration Guide.

## SAML SP SSO: Multi-tenancy support

Multi-tenancy support is added to FortiAuthenticator, where each tenant can be a FortiGate or a specific VDOM within a FortiGate:

- SAML SP SSO supports multiple SAML SP portals
- Each SAML SP portal can point to a different SAML IdP
- maintain multiple SSO sessions list
- each SSO session list contains the logged-in users for a set of domains
- each SSO session list has its own IP space
- IP spaces of different SSO session lists can overlap

## REST API enhancements

FortiAuthenticator sees the following REST API enhancements:

### Verify Security Question

Security question and password reset API is available for local and LDAP users. Using API calls, you can:

- set the password recovery question and answer
- read the password recovery question
- verify the password recovery answer
- reset the password

### Certificate management API

An API is added to manage user certificates. The API can be used to renew and revoke user certificates.

### REST API for syslog

RESTful API support is added for configuring syslog servers, and for configuring sending logs to a syslog server.

## Token self-provisioning by group option relocated

The option to allow token self-provisioning by user group is relocated to *Authentication* > *Self-service Portal* > *Token self-provisioning*. Token self-provisioning can also be configured from *Authentication* > *Guest Portals* > *Portals*.

## User Lookup

Administrators can perform a user search to easily monitor the ongoing activity of a specific user. The User Lookup page (*System* > *Dashboard* > *User Lookup*) provides a consolidated view of a user's information and recent activities.

## Automated Firmware Upgrade for HA A-P Clusters

When upgrading the firmware of the active unit in an HA master cluster, the administrator has the option to perform a coordinated upgrade of both cluster members. If BOTH is selected, the firmware upgrade is performed on the passive unit first. Once the first upgrade is complete and the passive unit backs up and syncs with the active unit, the firmware upgrade is performed on the active unit.

## Users Audit Report enhancements

Additional fields have been added to users audit reports. Reports now include fields that detail the date and time of account creation, date and time of last login, type of token-based authentication, and token information.

## Merge Captive Portal into Guest Portals

Captive Portals have merged with Guest Portals. Existing Captive Portals will convert to a Guest Portal configuration following a firmware upgrade. The look and function of converted portals will remain unchanged.

## SAML SP SSO: Select assertion for username

The SAML SP configuration offers administrators the option to specify which SAML assertion to extract the username from.

## SAML SP SSO: Disclaimer agreement page

When enabled, a SAML SP SSO end-user is required to agree to a disclaimer before being redirected to the SAML IdP for authentication. The disclaimer agreement page is enabled from the SAML Authentication page (*Fortinet SSO Methods* > *SSO*), and the disclaimer page is modified from the Replacement Messages page (*Authentication* > *Self-service Portal*).

## Wildcard MAC devices

When creating a new MAC-based authentication device (*Authentication* > *User Management* > *MAC Devices*), MAC addresses can be defined using wildcard capability to allow access to all devices from a specific manufacturer. Instead of defining a full MAC address, you define only the top 3 bytes (e.g. 11:22:33).

## HA maintenance mode

If maintenance needs to be performed on one of the FortiAuthenticator units in an HA master cluster, an administrator can use maintenance mode to remove the unit from the cluster. Maintenance mode is enabled from the High Availability page (*System* > *Administration*).

## Guest portals: Self-registration enhancements

FortiAuthenticator Guest Portals (*Authentication* > *Guest Portals* > *Portals*) are enhanced to improve the flexibility of the self-registration process. When configuring the self-registration pre-login services, administrators can:

- allow self-registration using only SMS or only email
- allow self-registration without SMS or email
- allow self-registrating users to select SMS or email

## Enhance FSSO DNS lookups

To improve FSSO DNS lookups, the behavior of the DNS cache on FortiAuthenticator can be configured under *System* > *Network* > *DNS*.

## Syslog matching rule for FortiNAC

FortiAuthenticator is preconfigured with a FSSO syslog matching rule for the FortiNAC. Syslog messages can be sent from the FortiNAC when there is a device register, login, or unregister event on the network, and the FortiAuthenticator can use these syslog messages for FSSO.

## VMware tools

The open-vm-tools package is integrated into the VMware-based FortiAuthenticator-VM. The VMWare tools package allows for additional features to be supported on the FortiAuthenticator-VM for the VMware server operator.

## NTP IPv6 support

Network Time Protocol (NTP) servers with an IPv6 address can be configured to synchronize the FortiAuthenticator system time.

## CA2 certificate support

Support is added for a second firmware certificate, signed by Fortinet's CA2 (FortiAuthenticator-VM only).

# Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator™ configuration, see the FortiAuthenticator Administration Guide.

## Hardware and VM support

FortiAuthenticator™ 5.5.0 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, and Xen)

## Deprecated hardware models

The following hardware models are EOS and are not supported in the FortiAuthenticator 5.5.0 release:

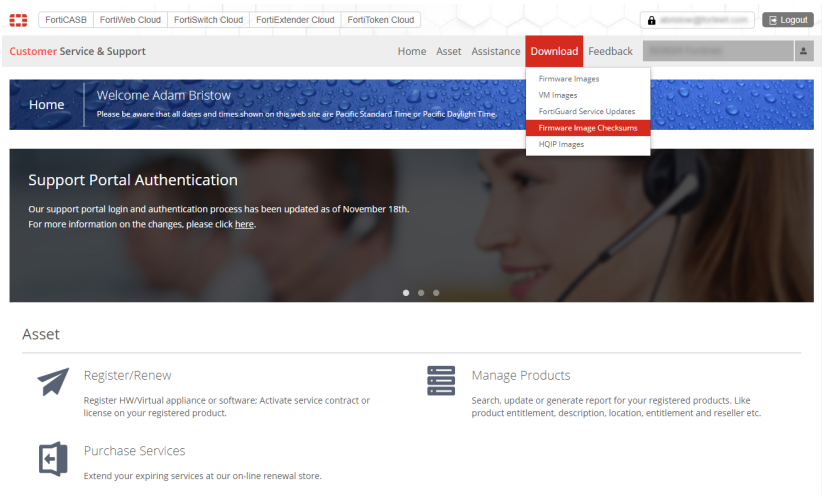
- FortiAuthenticator 3000B

## Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

### Customer service and support image checksum tool




After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

# Upgrading from FortiAuthenticator 4.x/5.x

FortiAuthenticator™ 5.5.0 build 0366 officially supports upgrade from all versions of FortiAuthenticator™ 4.x.x and 5.x.x.

Upgrading the FortiAuthenticator 3000D from 4.0.x to 4.1.x is not supported. The workaround for this model is to upgrade from any 4.0.x version directly to 4.2.0 or higher (skipping all 4.1.x versions).

If you install 4.1.x firmware on a FortiAuthenticator 3000D it stops responding. You can get the system running again by restoring valid firmware using the TFTP boot process.

## Firmware upgrade process

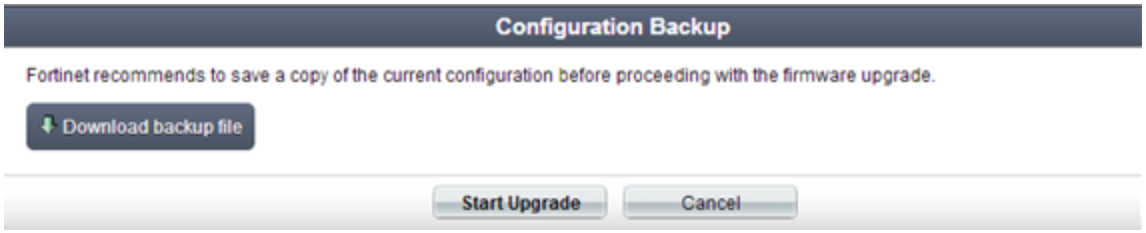
First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator™ firmware, you must download the firmware package from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator™ unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Go to **System > Dashboard > Status**.

5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. Select **OK** to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:




It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

# Product integration and support

## Web browser support

The following web browsers are supported by FortiAuthenticator™ 5.5.0:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 42
- Mozilla Firefox versions 61
- Google Chrome versions 70

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS support

FortiAuthenticator™ 5.5.0 supports the following FortiOS versions:

- FortiOS v6.0.3
- FortiOS v5.6.6
- FortiOS v5.4.10

The above versions have been verified by QA. Other FortiOS versions may function correctly, but may not be supported by Fortinet. Refer to the What's new section and Known Issues for version compatibility information.

## Fortinet agent support

FortiAuthenticator™ 5.5.0 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.2
- FortiAuthenticator Agent for Outlook Web Access 1.5
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

## Virtualization software support

FortiAuthenticator™ 5.5.0 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See Appendix A: FortiAuthenticator VM for more information.

## Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide.

# Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

| Bug ID | Description |
|---|---|
| **492709** | Downloading create_req.bat from the self-service portal leads to an error. |
| **509340** | IP address changes on existing SSO sessions take several minutes to be re-verified. |
| **501832** | Support for RADIUS secrets containing up to 64 characters. |
| **517217** | On an unlicensed FortiAuthenticator, new Captivate Portal replacement messages can not be created. |
| **472221** | Network Time Protocol (NTP) does not work via IPv6 interface. |
| **496580** | FortiAuthenticator intermittently returns HTTP 504 code after an API request to create a local user. |
| **503150** | When creating a new syslog SSO matching rule, certain characters can cause a GUI Unicode error when testing the rule. |
| **461429** | Unexpected Guest Portal user registration behavior with SMS. |
| **511548** | The ability to manage ping count and ping more than 4 times is missing. |
| **501629** | FortiAuthenticator loses FortiToken Mobile user association when using self-service portal. |
| **520394** | CLI commands that use FTP servers should support specifying port number. |
| **503717** | Migrations which uniquely rename duplicate objects should make sure new names don't collide. |
| **515315** | When the load-balancing slave is disconnected from the master for an extended period of time, the lb_sync process hangs permanently. |
| **519040** | When the load-balancing slave hasn't communicated with the master for more than one day, conflicts over token reassignment can arise. |
| **449801** | The GetCACert operation of a SCEP request logs an error that GetCACert has failed to retrieve the requested CA. |
| **467587** | The FQDN / CN comparison for admin GUI SSL certificate is case-sensitive. |
| **507766** | Through the API, push notifications are sent to disabled users. |

| Bug ID | Description |
|---|---|
| **439852** | When an interface is dedicated as HA management, it can still be edited in the CLI. |
| **512845** | When viewing a local user, the User created by FAS field should not be present. |
| **512925** | The HA Status page returns errors on the load-balancing slave. |
| **513576** | Push notifications are not sent for local users who override the default remote realm. |
| **397404** | The remote RADIUS user lockout code doesn't handle case sensitivity properly. |
| **512820** | Upgrade to OpenSSL 1.1.1 to permit support of TLS 1.3. |
| **508475** | On the SAML IDP Service Providers list, add a IdP Prefix column. |
| **442048** | On the Remote Users list page, the token link does note direct you to the FortiToken viewing page. |
| **504801** | In a HA-LB configuration, if you force a change password on next logon on the load-balancing slave, the changed password and 'force change password on next logon' will not be synced with the master. |
| **519353** | Incorrect validation check for MAC device description field when accessed via the user page. |
| **515066** | On the User Look page, page number links are present even when all users are displayed on the first page. |
| **506057** | Chained token authentication with remote RADIUS server causes an error with PCI in SAML. |
| **505907** | Remote Users with Chained token authentication with remote RADIUS server can't login to Guest Portal. |
| **486198** | Token Self-Provisioning doesn't work for remote users who belong to a group that uses an LDAP filter. |
| **512108** | When cloning a RADIUS client with profiles, you cannot make changes to the profiles and save them. |
| **504306** | Disassociating a FortiToken from a user with API Calls causes a GUI error to appear. |
| **504856** | When logging in via the GUI with a remote RADIUS user who has a FortiToken Mobile token assigned, the login attempt fails when accepting the push notification. |
| **508730** | After canceling password reset at Guest Portal, users have to enter credential twice in order to authenticate. |
| **505043** | In SAML IdP, if Force Password Change on next Login is enabled, the user is redirected to a login page with their username prepopulated. If Sign in as a different user is clicked, an error occurs. |

| Bug ID | Description |
|---|---|
| **499798** | If the ampersand symbol (&) is present in a randomly generated password sent out via SMS, it will display as '&'. |
| **503020** | The Reset Password page does not contain a Cancel button. |
| **504044** | Rephrase invalid token entry error message. |
| **517317** | Add assertion attribute support in SAML IdP for token authentication status. |
| **511947** | SSOMA/FSSO - support for <space> in usernames. |
| **514627** | When configuring the pre-login services for a Guest Portal, it is not possible to opt for randomly generated passwords to be sent via SMS. |
| **521798** | Token transfer fails and then the token data on the FortiAuthenticator becomes corrupted. |
| **521811** | Cluster high doesn't automatically switch back to master after maintenance mode set to on and then to off. |
| **517190** | FortiAuthenticator GUI isn't explicit regarding "enable authentication" for DC/TS Agents. |
| **518957** | FortiAuthenticator load-balancing slave issue causing users to be out of sync. |
| **509345** | Support for 2048 concurrent FortiClient FSSO connections. |
| **514662** | An error displays in the FortiAuthenticator certificate management CRL. |
| **507246** | FortiAuthenticator GUI login fails in Chrome and Firefox when two-factor authentication is used and the site is accessed via the FortiGate SSLVPN web portal. |
| **513174** | DH key exchange in EAP-TLS is using 1024 bit long modulus. |
| **503796** | A FortiAuthenticator acting as an FSSO collector agent does not detect workstation IP changes via DNS lookup. |
| **482913** | The information from authorityKeyIdentifier is not used to check the correct CRL for revocation status of user certificates. |
| **416807** | In the LDAP User Sync Mapping Preview window, some LDAP tree nodes that have children matching the test filter are not displayed as expected. |
| **504080** | Under certain conditions, FortiAuthenticator stops processing NTLM requests. |
| **438383** | FortiAuthenticator GUI displays a incorrect URL for CRL. |
| **519873** | A high rate of SAML Authentications will max out the Django CPU resources on the FortiAuthenticator. |

| Bug ID | Description |
|---|---|
| **508766** | The delay before being redirected to the please wait page for enabling/disabling HA scales up dramatically with the size of the database tables. |
| **519859** | Running load-balancing slave / load-balancing master in the foreground displays an OpenVPN insecure cipher warning. |
| **516350** | Load-balancing slaves can end up in a non-syncing state where they connect to cluster slave but not master. |
| **516354** | Load-balancing master and load-balancing slaves that have been upgraded from firmware version 5.0 or earlier are missing database functions. |
| **516349** | On FortiAuthenticator VMs, HA cluster salves can take longer to complete setup than currently permitted. |
| **516341** | HA cluster slave's failure to form cluster impacts availability of master. |
| **513965** | Permanent out-of-sync due to checksums for rows without data or syncable data without checksum on load-balancing master. |
| **512790** | Update Apple Push Notification Service certificates. |
| **508764** | Enabling or Disabling HA leads to frequent "An unexpected error has occurred" messages. |
| **508763** | The developer option to re-use existing configured interface for HA MGMT does not work. |
| **508761** | Using the CLI to add a route on the HA Management interface leads to an error. |
| **508526** | CVE-2018-5391 Linux kernel IP fragment re-assembly vulnerable to denial of service attacks. |
| **510379** | If tokens being transferred are in pending state, there is a probability that the transfer will fail. |
| **507391** | The data drive of a FortiAuthenticator-HyperV is created with a default size of 16GB instead of 60GB. |
| **506339** | An invalid SCEP request shouldn't produce internal server error. |
| **509520** | FortiAuthenticator should check for stray RADIUS client records in the database before attempting to clone an existing client. |
| **513454** | Transferred tokens produce error code 6 on FortiAuthenticator 5.4.0 GA build 0294. |

# Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

| Bug ID | Description |
|---|---|
| **502007** | The RADIUS accounting and CoA does not take effect on FortiAuthenticator. |
| **467883** | RDP users are prompted for credentials twice and fail the second prompt due to token reuse. |
| **519994** | When the sysOID is queried, FortiAuthenticator-VM identifies itself as a LINUX Net-SNMP agent system rather than a Fortinet device. |
| **521547** | Mobile phone numbers with seven or eight digits do not work with SMS Gateway. |
| **515429** | An error can cause loss of access to the FortiAuthenticator GUI. |
| **494705** | Domain authentication fails for users from trusted domains. |
| **520572** | When the pre-login disclaimer is enabled, the FSSO login widget requires two clicks instead of one. |
| **519319** | FortiAuthenticator-VM may crash when LDAP Remote user sync rules run. |
| **506294** | FortiAuthenticator truncates SSO groups in long SAML attributes resulting in log on failures. |
| **509936** | Under certain conditions, users are not removed from FortiAuthenticator when Remote user sync rule is executed. |
| **506112** | REST API call fails to activate FortiGuard Messaging license. |
| **512109** | When setting up SAML IdP, selecting a third-party server certificate that is still in a pending state causes a server crash. |
| **511093** | In a high availability setup, Radiusd on the load-balancing slave crashes if a large custom radius dictionary is uploaded to the master. |
| **519652** | Changing the FortiToken Mobile provisioning PIN length via REST API causes an internal server error. |
| **522057** | Deleting social users on the load-balancing slave causes slave to crash. |

# Appendix A: FortiAuthenticator VM

## FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported VM environment. For details, see the FortiAuthenticator VM Install Guide.

**VM requirements**

| Virtual machine | Requirement |
|---|---|
| VM form factor | Open Virtualization Format (OVF) |
| Virtual CPUs supported (minimum / maximum) | 1 / 8 |
| Virtual NICs supported (minimum / maximum) | 1 / 4 |
| Storage support (minimum / maximum) | 60GB / 2TB |
| Memory support (minimum / maximum) | 512 MB / 64GB |
| High Availability (HA) support | Yes |

## FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
  Use this image for new VM installations. It contains a deployable OVF virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, https://www.fortinet.com/products/identity-access-management.html#models-specifications.

# Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

## Hardware appliances

The following table describes the maximum values set for the various hardware models.

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| **System** | | | | | | |
| Network | Static Routes | 50 | 50 | 50 | 50 | 50 |
| Messages | SMTP Servers | 20 | 20 | 20 | 20 | 20 |
| | SMS Gateways | 20 | 20 | 20 | 20 | 20 |
| | SNMP Hosts | 20 | 20 | 20 | 20 | 20 |
| Administration | SYSLOG Servers | 20 | 20 | 20 | 20 | 20 |
| | User Uploaded Images | 30 | 100 | 500 | 1000 | 2000 |
| | Language Files | 50 | 50 | 50 | 50 | 50 |
| **Realms** | | 20 | 80 | 400 | 800 | 1600 |
| **Authentication** | | | | | | |
| General | Auth Clients (NAS) | 166 | 666 | 3333 | 6666 | 13333 |

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| | **Users** (Local + Remote)[1] | 500 | 2000 | 10000 | 20000 | 40000 |
| | User Radius Attributes | 1500 | 6000 | 30000 | 60000 | 120000 |
| | User Groups | 50 | 200 | 1000 | 2000 | 4000 |
| | Group Radius Attributes | 150 | 150 | 600 | 6000 | 120000 |
| | FortiTokens | 1000 | 4000 | 20000 | 40000 | 80000 |
| | FortiToken Mobile Licenses[2] | 200 | 200 | 200 | 200 | 200 |
| | LDAP Entries | 1000 | 4000 | 20000 | 40000 | 80000 |
| | Device (MAC-based Auth.) | 50 | 200 | 1000 | 2000 | 4000 |
| | RADIUS Client Profiles | 500 | 2000 | 10000 | 20000 | 40000 |
| | Remote LDAP Servers | 20 | 80 | 400 | 800 | 1600 |
| | Remote LDAP Sync Rule | 25 | 100 | 500 | 1000 | 2000 |
| | Remote LDAP User Radius Attributes | 1500 | 6000 | 30000 | 60000 | 120000 |
| **FSSO & Dynamic Policies** | | | | | | |
| FSSO | FSSO Users | 500 | 2000 | 10000 | 20000 | 200000[3] |
| | FSSO Groups | 1000 | 1000 | 5000 | 10000 | 20000 |
| | Domain Controllers | 10 | 20 | 100 | 200 | 400 |
| | RADIUS Accounting SSO Clients | 166 | 666 | 3333 | 6666 | 13333 |
| | FortiGate Services | 50 | 200 | 1000 | 2000 | 4000 |
| | FortiGate Group Filtering | 250 | 1000 | 5000 | 10000 | 20000 |
| | FSSO Tier Nodes | 5 | 20 | 100 | 200 | 400 |
| | IP Filtering Rules | 250 | 1000 | 5000 | 10000 | 20000 |

| Feature | | Model | | | | |
|---|---|---|---|---|---|---|
| | | 200E | 400E | 1000D | 2000E | 3000E |
| Accounting Proxy | Sources | 500 | 2000 | 10000 | 20000 | 40000 |
| | Destinations | 25 | 100 | 500 | 1000 | 2000 |
| | Rulesets | 25 | 100 | 500 | 1000 | 2000 |
| **Certificates** | | | | | | |
| User Certificates | User Certificates | 2500 | 10000 | 50000 | 100000 | 200000 |
| | Server Certificates | 50 | 200 | 1000 | 2000 | 4000 |
| Certificate Authorities | CA Certificates | 10 | 10 | 50 | 50 | 50 |
| | Trusted CA Certificates | 200 | 200 | 200 | 200 | 200 |
| | Certificate Revocation Lists | 200 | 200 | 200 | 200 | 200 |
| SCEP | Enrollment Requests | 2500 | 10000 | 50000 | 100000 | 200000 |

[1] Note that **Users** is the only metric used for the number of allowed users. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

## VM appliances

The FortiAuthenticator-VM Appliance is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM-Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

**100 / 10 = 10**

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

The following table describes the maximum values set for the various VM models.

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| **System** | | | | | |
| Network | Static Routes | 2 | 50 | 50 | 50 |
| Messaging | SMTP Servers | 2 | 20 | 20 | 20 |
| | SMS Gateways | 2 | 20 | 20 | 20 |
| | SNMP Hosts | 2 | 20 | 20 | 20 |
| Administration | SYSLOG Servers | 2 | 20 | 20 | 20 |
| | User Uploaded Images | 5 | Users / 20 | 5 | 100 |
| | Language Files | 5 | 50 | 50 | 50 |
| **Authentication** | | | | | |
| General | Auth Clients (NAS) | 3 | Users / 3 | 33 | 1666 |
| User Management | **Users** (Local + Remote)[1] | 5 | ********** | 100 | 5000 |
| | User RADIUS Attributes | 15 | Users x 3 | 300 | 15000 |
| | User Groups | 3 | Users / 10 | 10 | 500 |
| | Group RADIUS Attributes | 9 | Users x 3 | 300 | 15000 |
| | FortiTokens | 10 | Users x 2 | 200 | 10000 |
| | FortiToken Mobile Licenses (Stacked) [2] | 3 | 200 | 200 | 200 |
| | LDAP Entries | 20 | Users x 2 | 200 | 10000 |
| | Device (MAC-based Auth.) | 1 | Users / 10 | 10 | 500 |

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| | RADIUS Client Profiles | 3 | Users | 100 | 10000 |
| | Remote LDAP Servers | 4 | Users / 25 | 4 | 200 |
| | Remote LDAP Sync Rule | 1 | Users / 10 | 10 | 500 |
| | Remote LDAP User Radius Attributes | 15 | Users x 3 | 300 | 15000 |
| **FSSO & Dynamic Policies** | | | | | |
| FSSO | FSSO Users | 5 | Users | 100 | 5000 |
| | FSSO Groups | 30 | Users / 2 | 50 | 2500 |
| | Domain Controllers | 3 | Users / 100 (min=10) | 10 | 50 |
| | RADIUS Accounting SSO Clients | 10 | Users | 100 | 5000 |
| | FortiGate Services | 2 | Users / 10 | 10 | 500 |
| | FortiGate Group Filtering | 30 | Users / 2 | 50 | 2500 |
| | FSSO Tier Nodes | 3 | Users /100 (min=5) | 5 | 50 |
| | IP Filtering Rules | 30 | Users / 2 | 50 | 2500 |
| Accounting Proxy | Sources | 3 | Users | 100 | 1000 |
| | Destinations | 3 | Users / 20 | 5 | 250 |
| | Rulesets | 3 | Users / 20 | 5 | 250 |
| **Certificates** | | | | | |
| User Certificates | User Certificates | 5 | Users x 5 | 500 | 25000 |
| | Server Certificates | 2 | Users / 10 | 10 | 500 |

| Feature | | Model | | | |
|---|---|---|---|---|---|
| | | Unlicensed VM | Calculating metric | Base VM (100 users) | Example 5000 licensed user VM |
| Certificate Authorities | CA Certificates | 3 | Users / 20 | 5 | 250 |
| | Trusted CA Certificates | 200 | 200 | 200 | 200 |
| | Certificate Revocation Lists | 5 | 200 | 200 | 200 |
| SCEP | Enrollment Requests | 5 | Users x 5 | 2500 | 10000 |

[1] Note that there is one metric used for the number of allowed users which is **Users**. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.